

Risk Assessment of Processor- Based Signal & Train Control Systems

RSAC Panel
on Risk Assessment

May 14, 2002

John Wreathall

The WreathWood Group
Consultants to Volpe Center

The WreathWood Group

Background in Risk Assessment

- Work on risk and reliability modeling in nuclear submarine safety (UK, 1975+)
- PRA studies for 15 nuclear plants, aerospace, chemical & military systems
- NRC reviewers of HRA portions of ~20 Individual Plant Examination (IPE) submittals
- Evaluations of medical, chemical plant, aviation & maritime errors
- Developers of numerous HRA & PRA methods

What is a Risk Assessment?

Fault Trees
Event Trees
FMECAs
PHAs
Event Sequence Diagrams
HAZOPs
Simulation
GO Models
Markov Process

Art
Logic Modeling
Mechanistic Calculations

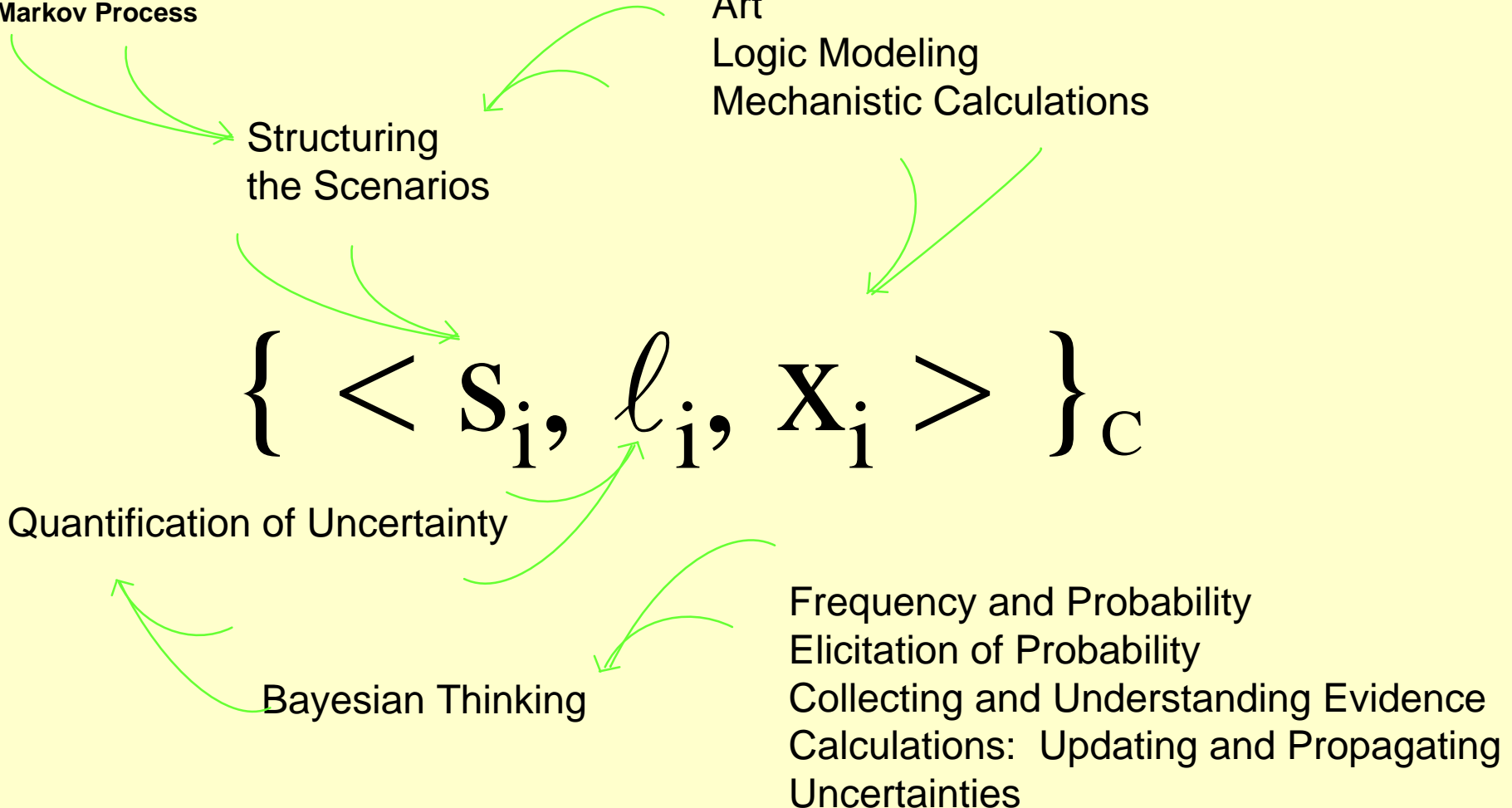
Structuring
the Scenarios

$$\{ \langle s_i, \ell_i, x_i \rangle \}_c$$

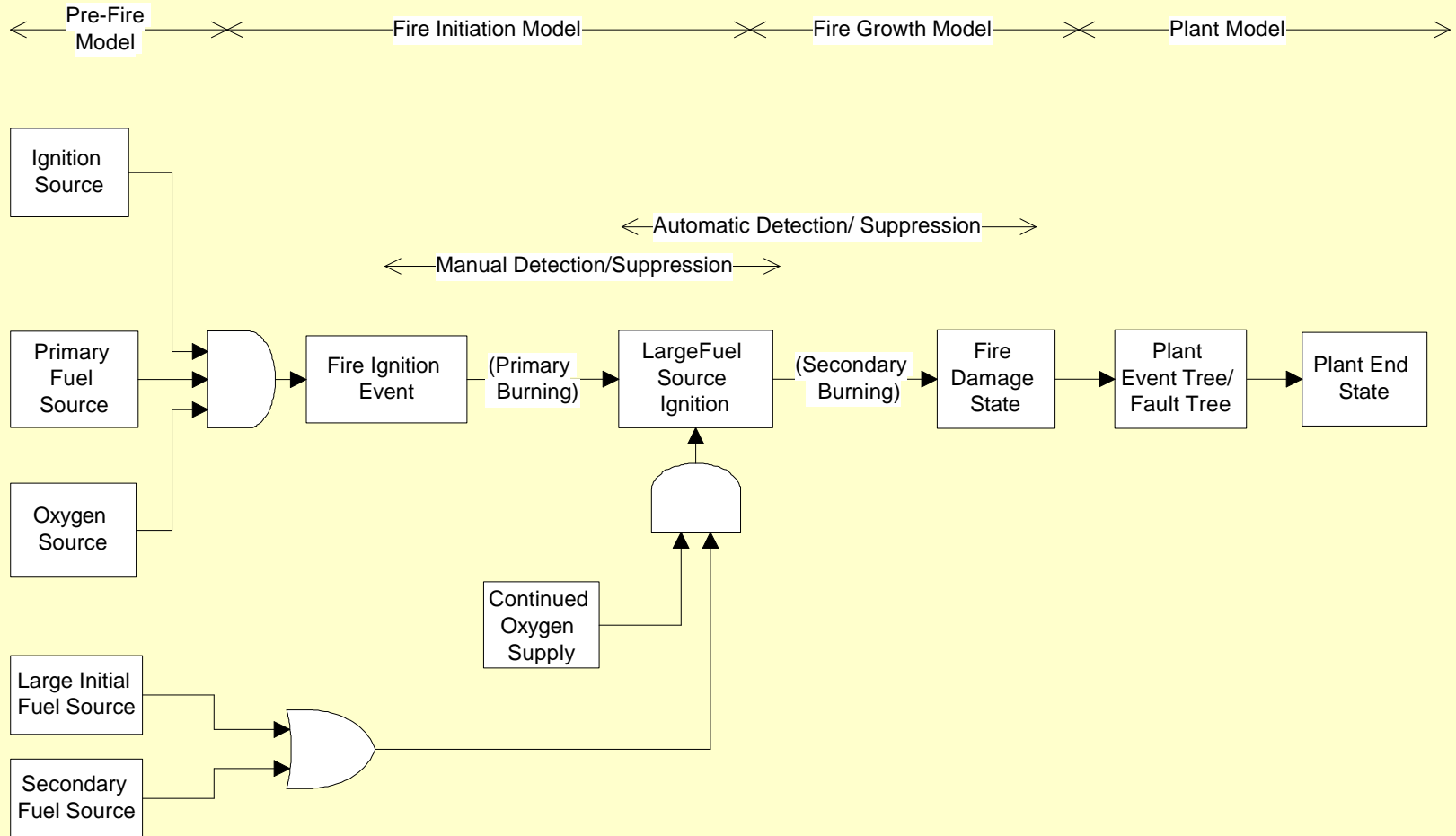
Quantification of Uncertainty

Bayesian Thinking

Frequency and Probability
Elicitation of Probability
Collecting and Understanding Evidence
Calculations: Updating and Propagating
Uncertainties



Structure of a Fire Risk Model



Pro's & Con's of Risk Assessment

Pro's

- Common dimension for decisions
- Provides a framework for combining many different types of analyses
- Gives detailed understanding of contribution to risks & how to fix
- Uncertainties, sensitivities can be analyzed
- Scaleable to budget (somewhat)

Con's

- Not all issues can be modeled explicitly
- Methods can be “tricky” for human, organizational contributions
- “You get what you pay for”





Characteristics of a Satisfactory PRA (& HRA) Method

1. It is useable for resolving the issue(s) at hand
2. It is simple, consistent with the needs of (1)
3. It can provide satisfactory explanations for its results
4. Its results and explanations are adequately consistent with historical experience within the context of the issues of (1)
5. It is capable of withstanding scrutiny and review
6. It is capable of being updated or revised with new experience (data or knowledge)

Examples of Risk Analysis Techniques

- Nuclear power plant at power: high consequence/rare events—*event tree/fault tree for scenarios, various HRA, simulation for consequences (dispersion and dose)*
- Nuclear power plant decay heat: high conseq/rare—*phased mission event tree/fault tree, HRA focused on dependencies and context*
- Space shuttle: high conseq/rare—*phased mission event tree/fault tree*
- Chemical weapons destruction facility: med-high conseq/rare—*plant operational diagrams, event tree/fault tree for scenarios, various HRA, simulation for consequences (dispersion and dose)*
- Electric power plant reliability: low-med conseq/routine—*simulation*
- Medical misapplication: individual high conseq/occasional—*HRA focused on organizational factors*

Relationship of PRA with Proposed Rule Requirements

- Need to compare safety before & after change in design 
- Handles integrated systems view 
- Need to document assumptions, including human performance 
- Risk-informed regulatory decisionmaking, not risk-based 

The End